

JPW



PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	10/709,423
	Filing Date	05/05/2004
	First Named Inventor	Chih-Chung Lu
	Art Unit	
	Examiner Name	
Total Number of Pages in This Submission	3	Attorney Docket Number IEIP0012USA

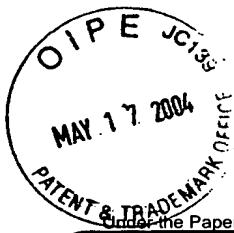
ENCLOSURES (Check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input checked="" type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/Incomplete Application <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation <input type="checkbox"/> Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____	<input type="checkbox"/> After Allowance communication to Technology Center (TC) <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below):
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Winston Hsu, Reg. No.: 41,526
Signature	<i>Winston Hsu</i>
Date	5/13/2004

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.			
Typed or printed name			
Signature		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 0.00

Complete if Known

Application Number 10/709,423
Filing Date 05/05/2004
First Named Inventor Chih-Chung Lu
Examiner Name
Art Unit
Attorney Docket No. IEIP0012USA

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number 50-3105
Deposit Account Name North America Intellectual Property Corp.

The Director is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	
SUBTOTAL (1)					(\$) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims	Fee from below	Fee Paid
Total Claims		-20** =	X	
Independent Claims		-3** =	X	
Multiple Dependent				

Large Entity		Small Entity		Fee Description
Fee Code	Fee (\$)	Fee Code	Fee (\$)	
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Small Entity

Fee Code	Fee (\$)	Fee Code	Fee (\$)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for ex parte reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	0.00
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$) 0.00

SUBMITTED BY

(Complete (if applicable))

Name (Print/Type) Winston Hsu Registration No. 41,526 Telephone 886289237350
Signature [Signature] (Attorney/Agent) Date 5/13/2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



PTO/SB/02B (11-00)

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

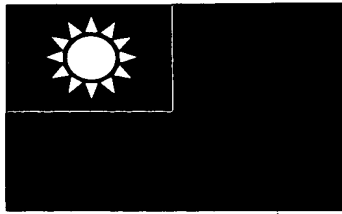
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
092137360	Taiwan R.O.C	12/30/2003	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2003 年 12 月 30 日
Application Date

申請案號：092137360
Application No.

申請人：威達電股份有限公司
Applicant(s)

局長
Director General

蔡練生

發文日期：西元 2004 年 3 月 12 日
Issue Date

發文字號：09320239280
Serial No.

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：

※ 申請日期：

※IPC 分類：

壹、發明名稱：(中文/英文)

加速封包過濾之方法

A Method for speeding packet filter

貳、申請人：(共 1 人)

姓名或名稱：(中文/英文)

1.威達電股份有限公司/ ICP electronic Inc.

代表人：(中文/英文) 郭博達

住居所或營業所地址：(中文/英文)

台北縣 221 汐止市中興路 22 號 3 樓

3F, NO.22, Chung-Hsing Rd., Shi-Chi City, Taipei Hsien, 221, Taiwan,
R.O.C.

國 籍：(中文/英文) 中華民國/R.O.C.

參、發明人：(共 1 人)

姓 名：(中文/英文)

1.呂致中/ LU, CHIH-CHUNG

住居所地址：(中文/英文)

1.台北市 105 敦化北路 145 巷 18 號 2 樓

國 籍：(中文/英文) 中華民國/R.O.C.

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

伍、中文發明摘要：

一種加速封包過濾之方法，係以一搜尋過濾器搭配網路防火牆內之規則，該方法包括：依據防火牆規則在一第一赫序空間上呈現所有欲過濾網段的特徵值集合，且依據收到的封包在一第二赫序空間呈現該封包之網址特徵值集合，進而將相同大小的第一及第二赫序空間進行特定的布林運算，一旦結果判斷出該封包特徵值集合不在該網段特徵值集合之範圍內，即迅速允許該封包通過該防火牆，藉此更可以縮短計算時間、降低系統負載及避免網路壅塞。

陸、英文發明摘要：

柒、指定代表圖：

(一)本案指定代表圖為：第(4)圖。

(二)本代表圖之元件代表符號簡單說明：

操作步驟 S600, S605, S610, S615, S620, S625, S630, S640,
S645

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

玖、發明說明：

【發明所屬之技術領域】

一種加速封包過濾之方法，特別一種採用搜尋過濾器原理以協助防火牆加速過濾封包之方法。

【先前技術】

目前網路科技的日新月異促使大量的資料可在瞬間傳遞於世界各地之間，但相對的，如何提昇網路安全也變成極重要的課題，在一般完整的網路系統中，一些連接網路主幹的網路設備如虛擬私有通道網路(VPN)、閘道器(GATEWAY)或路由器(ROUTER)等，大多具有網路防火牆(FIREWALL)或甚至獨立設置。此類網路防火牆的設計主要集中在網路層(IP Layer)上的保護，也就是提供一種封包過濾(packet filter)的機制，其原理是利用使用者預設的每一條防火牆規則(FIREWALL RULE)去比對每一個流經該防火牆的外來封包。然而，事實上每一防火牆規則即代表一搜尋成本包括如搜尋時間成本、系統負載成本及人力設計成本，該防火牆規則設計越多、規則定義得越繁瑣或範圍越廣，雖然使搜尋的準確度提高，但相對花費的搜尋成本也非常高，如果因封包處理時間過長反而造成整個網路系統效能下降或甚至壅塞，這樣的設計並無任何存在的價值；反之，過於考量最低搜尋成本而減少防火牆規則或範圍，卻又可能使防火牆的防護功能下降。因此防火牆的效能之一就是在具有最低搜尋成本的防火牆規則之情況下，但又能兼具封包搜尋的準確度。

習知封包過濾之方法即判定一個外來封包是否為防火牆規則定義的範圍所涵蓋，其中最常使用方法就是一種線性搜尋(linear search)，亦即用一個一個防火牆規則逐一比對收到的封包。此外，已有一些改進的方法是利用一些已知的搜尋演算法應用於封包過濾的過程中，以專門搜尋有問題或有害的封包。但實際運作時，防火牆收到的封包大部份都不在防火牆規則

定義的範圍內，是屬於”良性或無害”的封包，也就是說大部分的封包都可以順利通過防火牆的過濾。相對的，其意謂著大多數的搜尋演算法皆是將大部份的搜尋成本如時間，花費在一些根本不需要過濾的封包上。

有鑑於前述習知技術之缺點，發明人採逆向思考認為如果在進行封包搜尋之前，應用一具極小成本的搜尋方法，先找出大部份非屬欲過濾之良性封包並讓其通過，而僅留少部份有問題的封包以傳統搜尋方法檢查，如此可大大減低搜尋成本，如系統負載降低、搜尋時間加快，而且無需更改任何原有的防火牆規則。

是以，本發明利用一種搜尋過濾器(search filter)的概念以達成上述解決方法。所謂「搜尋過濾器」是 Severance 和 Lohman 在 1976 年所提出來一種專門搜尋文字或文件的方法，其原理為：先選出一些赫序函數或稱散列函數(Hash function)如 MD5，並以欲搜尋的數值如 m 作為該赫序函數之鍵值(Key)如 $f(m)$ 以進行赫序函數運算，進而得到一適當的資料結構排列，之後即可將該資料結構用於篩選欲檢查的數值。當有一鍵值被篩選出來時，依據搜尋過濾器的特性，是不能保證該鍵值(Key)就一定可以在搜尋集合中找到，這是因為搜尋過濾器所使用的赫序空間(hash space)有限；反之，當有一被篩選出來不屬於搜尋集合的鍵值時，該搜尋過濾器就可以確定該鍵值一定不屬於搜尋集合。

【發明內容】

本發明之一主要目的在於提供一種加速封包過濾之方法，其利用前述搜尋過濾器的原理，使網路防火牆在進行封包搜尋之前，以極小的運算和空間成本，先迅速篩選出大部份無害封包並讓其通過，而僅有少數有問題之封包才會被具較高搜尋成本之其他搜查過濾機制直接處理，藉使防火牆將可節省大量運算時間、避免網路壅塞及提昇防火牆之過濾效率，且降低系統之運算負載。

為達上述目的，依據本發明之一種加速封包過濾之方法，係以一搜尋過濾器搭配網路防火牆之規則，該方法包括：

將至少一防火牆規則之特定網段轉換成以二位進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一相對位址分別轉換成一指
向第一赫序空間之對應位址，藉以取得該特定網段之指向第一赫序空間之
對應位址的集合；

收集所有指向第一赫序空間之對應位址的集合，以在該第一赫序空間
中呈現出所有欲過濾網段之特徵值集合；

將該防火牆所收到每一封包內之特定網址轉換成以二位進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一相對位址分別轉換成一指
向第二赫序空間之對應位址，藉以取得該網址之指向第二赫序空間之對應
位址的集合，其中該第二赫序空間大小與前述第一赫序空間相同；

收集所有指向第二赫序空間之對應位址的集合，以在一第二赫序空間
中呈現出該封包之網址特徵值集合；以及

進而將相同大小的第一及第二赫序空間進行特定的布林運算，一旦結
果判斷出該封包特徵值集合不在該網段特徵值集合之範圍內，即迅速允許
該封包通過該防火牆。

【實施方式】

請見第 1 圖，係依據本發明之較佳實施例之一種加速封包過濾之方法
係利用一搜尋過濾器(search filter)24 應用於一網路安全裝置如防火牆 20
中，以配合該防火牆 20 中預設的複數個防火牆規則 22 之封包過濾工作。
前述防火牆 20 可如第 1 圖所示連接於一網際網路(Internet)10 及一區域網路
系統(LAN)30 之間，以過濾經由該網際網路 10 傳來的所有外來封包，其中
經過過濾無問題的封包方能進入該區域網路系統(LAN)30 中。

利用前述搜尋過濾器之原理，本發明之加速封包過濾之方法，包括如
下：

1.一種產生所有欲過濾網段特徵值集合(mask characteristic value set)方

法：

(1)預設條件：

(a)假設第 1 圖所示之防火牆 20 中具有 N 條防火牆規則 $\{1 \leq i \leq N \mid r_i\}$ ，其中每一條規則 r_i 包含五個欄位： $\{\text{來源網段}(\text{source network}) r_{i\text{net}_s}, \text{目的網段}(\text{destination network}) r_{i\text{net}_d}, \text{來源埠}(\text{source port}) r_{i\text{port}_s}, \text{目的埠}(\text{destination port}) r_{i\text{port}_d}, \text{通訊協定}(\text{protocol}) r_{ip}\}$ 。前述規則 r_i 中所描述的每一個網段代表包含使用者欲過濾去除的 IP 網址。

(b)預設 K 個獨立的赫序函數 $h_i \{1 \leq i \leq K\}$ ，(例如有兩個赫序函數 h_1 及 h_2 互為獨立，即不保證當 $m \neq m'$ 時，則 $h_1(m) \neq h_2(m')$)，作為之後產生一赫序函數空間 H 的邏輯運算。

(c)需注意的是，本發明方法之過濾準確度受限於預設的赫序空間大小與所選擇赫序函數的特性有關。此外，前述搜尋過濾器之效能可以一硬體或為一軟體之形成來達成。

(2)方法流程：

首先進行如第 2 圖之步驟 S400 所示，先定義每一赫序空間(Hash Space)所佔用的大小=每一個赫序函數 h_i 的輸出定址空間大小= $C * K * L$ ，其中 C 為一個自定的常數，而 L 為 IP 位址以二進位表示法所需佔用之位元數，以 IPV4 為例，則 $L=32$ 。

如步驟 S405 所示，先自每一條防火牆規則 r_i 中取出一來源網段 $r_{i\text{net}_s}$ ；步驟 S410，將該來源網段 $r_{i\text{net}_s}$ 轉換成以二進位碼排列表示(包括位元值及相對位址)；步驟 S415，自前述來源網段 $r_{i\text{net}_s}$ 之二進位碼排列中，找出位元值(bit)為"1"的 M 個相對位址 $b_m (0 \leq b_m \leq L-1, 0 \leq m \leq M-1)$ 之集合；步驟 S420，將該每一二進位碼位元值為"1"之位址、來源埠 $r_{i\text{port}_s}$ 及通訊協定編號 r_{ip} 作為赫序函數之鍵值(Key)，分別帶入 K 個特定赫序函數 h_i 如 $h_i(b_m, r_{i\text{port}_s}, r_{ip})$ 中進行赫序運算，以求出 $K * M$ 個介於 0 到 $(C * K * L) - 1$

的值 k_j ，此值 k_j 即為該來源網段之每一指向一赫序空間 H_s 的相對位址，藉此如步驟 S425 所述，前述指向一赫序空間 H_s 的相對位址之集合可在此一赫序空間 H_s 上呈現該來源網段 r_{inet_s} 之特徵值分佈。惟，前述赫序函數之鍵值取樣是可以自定，但最少要採用該位元值為"1"之二進位碼位址、來源埠 r_{iport_s} 及通訊協定編號 r_{ip} 三者其中之一作為前述赫序函數之鍵值，如僅採用該網段之位元值為"1"的二進位碼位址作為鍵值。

相同於前述該來源網段 r_{inet_s} 的過濾過程，如對同一條防火牆規則 r_i 中之目的網段 r_{inet_d} 的過濾過程也是重覆前述步驟 S400 至 S250 之動作，即先轉換成以二進位碼排列，再將該二進位碼排列中每一位元值(bit)為"1"的 W 個位址 b_w ($0 \leq b_w \leq L-1$, $0 \leq w \leq W-1$)、目的埠 r_{iport_d} 及通訊協定編號 r_{ip} 三者作為赫序函數之鍵值(Key)，分別帶入前述 K 個赫序函數 h_i 如 $h_1(b_w, r_{iport_d}, r_{ip})$ 中進行赫序運算，以求出 $K*W$ 個介於 0 到 $(C*K*L)-1$ 的值 k_j ，此值 k_j 即包括該目的網段 r_{inet_d} 之每一指向一赫序空間 H_d 的相對位址，藉由該指向赫序空間 H_d 的相對位址之集合可在此赫序空間 H_d 上呈現出該目的網段 r_{inet_d} 之特徵值。需注意的是，因為每一赫序空間使用的 C 、 K 及 L 值皆相同，所以前述赫序空間 H_d 之空間大小必定等於赫序空間 H_s 之空間大小，亦等於其他赫序空間之空間大小。

接著如步驟 S435 及步驟 S440 所示，重複對 N 條防火牆規則之網段(包括來源網段及目的網段)進行與上述相同之運算，即可分別得到複數個赫序空間 H_d 及 H_s ；再如步驟 S430，收集該 N 條防火牆規則中所有欲過濾網段指向赫序空間 H 的相對位址之集合，即將所有前述複數個赫序空間 H_d 及 H_s 中同一位址之位元值進行加總運算，以在同一赫序空間 H (即 $H=H_d+H_s$) 上可呈現所有 N 條防火牆規則中欲過濾網段之特徵值總合(characteristic value sum)。

步驟 S445，進一步將前述網段特徵值總合之赫序空間 H 中非屬"0"

的位元值改設為"1"；相反的，如位元值為"0"者，則仍保留為"0"，藉此如步驟 S450，最後可在同一赫序空間 H 上得到的這 N 條防火牆規則的網段特徵值集合(characteristic value set)。

2. 一種產生封包網址特徵值集合(Packet characteristic value set)之方法：

(1)預設條件：假設每一個欲檢查的資料封包 p 包括： $\{\text{來源網址 } \text{pip}_s, \text{目的網址 } \text{pip}_d, \text{來源埠 } \text{pport}_s, \text{目的埠 } \text{pport}_d, \text{通訊協定 } \text{pp}\}$ ，且處理封包之方法與對前述網段之處理方法類似，即定義另一赫序空間 H' 大小=前述赫序空間 H 大小= $C*K*L$ 的記憶空間，並將其中每一個位元內容清除為 0，以及使用相同的 K 個赫序函數 $h_i \{1 \leq i \leq K\}$ 。

(2)方法流程：

首先如步驟 S550，收到一個欲檢查的資料封包 p；步驟 S505，自該封包中取出一來源網址 pip_s ；步驟 S510 將該封包之來源網址 pip_s 轉換成以二進位碼排列表示；步驟 S515，自該二進位碼排列中找尋位元值(bit)為"1"的 M' 個位址 $b'_m (0 \leq b'_m \leq L-1, 1 \leq m \leq M'-1)$ 之集合；步驟 S520，將每一二進位碼中位元值為"1"的位址、來源埠 pport_s 及通訊協定編號 pp 作為赫序函數之鍵值(Key)，分別帶入同樣是 K 個赫序函數 h_i 如 $h_1(b'_m, \text{pport}_s, \text{pp})$ 中運算，求出 $K*M'$ 個介於 0 到 $(C*K*L)-1$ 的值 k_j ，此值 k_j 即包括該來源網址 pip_s 之每一指向一赫序空間 H'_s 的相對位址，藉此如步驟 S525 所示，利用該指向一赫序空間 H'_s 的相對位址之集合即可在此赫序空間 H'_s 上呈現此封包之來源網址 pip_s 特徵值。

基於同樣原理，如將該封包之目的網址 pip_d 、目的埠 pport_d 及通訊協定編號 pp 作為赫序函數之鍵值(Key)進行 K 個赫序函數的運算，即將封包之目的網址 pip_d 轉換成指向一赫序空間 H'_s 的相對位址之集合，藉此可在此赫序空間 H'_d 上呈現此封包之目的網址 pip_d 特徵值。

步驟 S535，對同一封包中之其他 IP 位址重覆進行運算；步驟 S530，

收集該封包之所有網址指向赫序空間 H'_s 的相對位址之集合，即將所有前述赫序空間 H'_s 及 H'_d 中屬同一位址之位元值進行加總運算，以在一赫序空間 H' ($H'=H'_s+H'_d$) 上呈現這封包之所有網址特徵值總合(packet characteristic value sum)；步驟 S540，再將該赫序空間 H' 中非"0"的位元值皆改設為"1"， $0 \leq j \leq (K*M')-1$ ；步驟 S545，在此赫序空間 H' 上呈現該封包特徵值集合(packet characteristic value set)。

接著進行步驟 S550，進行一布林運算檢查，即在同一的赫序空間中，以前述欲過濾網段之特徵值集合比對該封包之欲檢查網址特徵值集合，以判定該封包特徵值集合是否不在前述網段特徵值集合之內。

3.運算檢查之方法：

首先如步驟 S600 及 S605，已分別獲得一具網段特徵值集合之赫序空間 H 及一具封包特徵值集合之赫序空間 H' ；步驟 S610 及 S615，進行下列布林運算：

$$(H \text{ OR } H') \text{ XOR } H$$

步驟 S620，判斷前述布林運算之結果，若全部位元皆為"0"，即如步驟 S640，該封包 p 所載之 IP 位址有可能為該 N 條防火牆規則之網段特徵值集合所涵蓋，應該進一步如步驟 S645 所示，再搭配其他具深度的搜尋機制(具較高搜尋成本)確認是哪一個規則或過濾此封包；反之，若步驟 S620 之判斷結果為至少有一位元不為"0"，則如步驟 S625 所示，代表則該封包 p 所載之 IP 位址一定不為該 N 條防火牆規則之網段特徵值集合所涵蓋，即進行步驟 S630，允許該封包通過防火牆。

需注意的是，若有任何防火牆規則的增/減，則先求出該規則在赫序空間的特徵值 H_c ，之後該具網段特徵值總合之赫序空間即為 $H=H-H_c$ 或 $H=H+H_c$ ，再運算出新的網段特徵值集合。如果是防火牆規則的修改，則仿照先減去舊的規則在新增新的規則之方式得到新的網段特徵值集合。

假設有一防火牆具有兩條防火牆規則(即 $N=2$)如下:

順序	來源網段	來源埠	目的網段	目的埠	協定	行動
1	12.0.0.0/24	0	202.1.237.21/32	80	1	Accept
2	12.0.0.0/24	0	172.17.23.152/29	23	1	Accept

(其中通訊埠為"0"代表任意埠)

另假設一預設常數 $C=2$ 、每一 IP 位址所使用的位元大小 $L=32$ 以及兩個互相獨立的赫序函數 $\{1 \leq i \leq 2 \mid h_i\}$ (即 $K=2$)，則每一赫序空間 H 大小=每一個赫序函數 h_i 的輸出定址空間大小 $=C*K*L=2*2*32=128$ bit，並將其中每一個位元內容清除為 0，即：

赫序空間 H

[illegible]

自第一條防火牆規則中取出一來源網段 r_1net_s (即 12.0.0.0/24)，並將該來源網段轉換成以二進位碼排列如下：

位址	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
位元	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

從上述之來源網段 r_1net_s 之二進位碼排列中找尋位元值之"1"的 M 個相對位址之集合，因此從上可知： $M=10$ ，該相對位址集合= $\{b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9\}=\{0, 1, 2, 3, 4, 5, 6, 7, 26, 27\}$

將上述每一二進位碼位元值為"1"之相對位址{0,1,2,3,4,5,6,7,26,27}、來源埠 r_{iport_s} (即 0)及通訊協定編號 r_{ip} (即 1)作為赫序函數之鍵值(Key)，以分別帶入 2 個赫序函數 h_i 以分別求得下列 20 個(M x K)指向一赫序空間 H_{1s} 的位址之集合：

$$\begin{aligned} h_1(0,0,1) &= 41, h_1(1,0,1) = 111, h_1(2,0,1) = 41, h_1(3,0,1) = 39, \\ h_1(4,0,1) &= 100, h_1(5,0,1) = 42, h_1(6,0,1) = 1, h_1(7,0,1) = 21, \\ h_1(26,0,1) &= 92, h_1(27,0,1) = 4 \end{aligned}$$

$$\begin{aligned} h_2(0,0,1) &= 21, h_2(1,0,1) = 41, h_2(2,0,1) = 40, h_2(3,0,1) = 1, \\ h_2(4,0,1) &= 98, h_2(5,0,1) = 120, h_2(6,0,1) = 12, h_2(7,0,1) = 88, \\ h_2(26,0,1) &= 76, h_2(27,0,1) = 110 \end{aligned}$$

依上述 20 個指向赫序空間 H_{1s} 之位址的集合，如下所示在此赫序空間 H_{1s} 上呈現一第 1 條防火牆規則之來源網段特徵值：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	

再自同一第一條防火牆規則中取出一目的網段 r_{inet_d} (即 202.1.237.21/32)，並將該目的網段 r_{inet_d} 轉換成以二進位碼排列如下：

位址	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
位元	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	0	1	0	0	0	1	0	1	0	1

從上述目的網段 r_{inet_d} 之二進位碼排列中找尋位元值之"1"的 W 個相對位址之集合，因此從上可知： $W=14$ ，是以，該相對位址集合= $\{b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{13}\}=\{0,2,4,8,10,11,13,14,15,16,25,27,30,31\}$

將上述每一二進位碼位元值為"1"之相對位址 $\{0,2,4,8,10,11,13,14,15,16,25,27,30,31\}$ 、目的埠 r_{ipport_d} (即 80)及通訊協定編號 r_{ip} (即 1)作為赫序函數之鍵值(Key)，以分別帶入 2 個赫序函數 h_i 以分別求得下列 28 個($K \times W$)指向一赫序空間 H_{ld} 的位址之集合：

$$\begin{aligned} h_1(0,80,1) &= 50, h_1(2,80,1) = 76, h_1(4,80,1) = 43, h_1(8,80,1) = 66, \\ h_1(10,80,1) &= 9, h_1(11,80,1) = 12, h_1(13,80,1) = 21, h_1(14,80,1) = 36, \\ h_1(15,80,1) &= 61, h_1(16,80,1) = 58, h_1(25,80,1) = 81, h_1(27,80,1) = 108, \\ h_1(30,80,1) &= 52, h_1(31,80,1) = 12 \end{aligned}$$

$$\begin{aligned} h_2(0,80,1) &= 20, h_2(2,80,1) = 67, h_2(4,80,1) = 7, h_2(8,80,1) = 96, \\ h_2(10,80,1) &= 12, h_2(11,80,1) = 84, h_2(13,80,1) = 61, h_2(14,80,1) = 29, \\ h_2(15,80,1) &= 17, h_2(16,80,1) = 77, h_2(25,80,1) = 20, h_2(27,80,1) = 99, \\ h_2(30,80,1) &= 121, h_2(31,80,1) = 41 \end{aligned}$$

依上述 28 個指向赫序空間 H_{ld} 的位址之集合，在此赫序空間 H_{ld} 上呈現一呈現第 1 條防火牆規則之目的網段特徵值，進而收集第 1 條防火牆規則之所有網段指向一赫序空間 H 的位址之集合，即將該兩赫序空間 H_{ld} 及 H_{ls} 中屬同一位址之位元值進行加總運算，以在此赫序空間 $H(H=H_{ls}+H_{ld})$ 上呈現一第 1 條防火牆規則之網段特徵值總合：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	1	0	0	1	0	0	1	0	1	0	0	4	0	0	0	0	1	0	0	2	2	0	0	0	0	0	0	0	1	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	0	0	1	0	0	1	1	2	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	2	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	1	1	0	0	0	0	0	0	0	0	2	1	0	0	0	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	1	0	1	1	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0

自第二條防火牆規則中取出一來源網段 r_2net_s (即 12.0.0.0/24)，但因該來源網段 r_2net_s 與前述來源網段 r_1net_s 相同，故不再贅述其赫序函數之運算過程，而直接將其赫序空間 H_{2S} 加入前述赫序空間 H 中作位元累加，因此赫序空間 $H = H + H_{2S}$ ，其呈現的網段特徵值總合如下所示：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	2	0	0	2	0	0	1	0	1	0	0	5	0	0	0	0	1	0	0	2	3	0	0	0	0	0	0	0	1	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	0	0	1	0	0	2	2	3	2	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	2	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	1	1	0	0	0	0	0	0	0	0	3	1	0	0	0	1	0	0	1	0	0	0	2	0	0	0	2	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	1	0	2	1	2	0	0	0	0	0	0	0	1	0	2	2	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0

再自第 2 條防火牆規則中取出一目的網段 r_2net_d (即 172.17.23.152/29)，並將該目的網段 r_2net_d 轉換成以二進位碼排列如下：

位址	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
位元	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	1	1	1	1	0	0	1	1	1	1	1

從上述目的網段 r_2net_d 之二進位碼排列中找尋位元值之"1"的 W 個相對位址之集合，因此從上可知： $W=16$ ，是以，該相對位址集合= $\{b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{14}, b_{14},$

$b_{15}\}=\{0,1,2,3,4,7,8,9,10,12,16,20,26,27,29,31\}$

將上述每一二進位碼位元值為"1"之相對位址
 $\{0,1,2,3,4,7,8,9,10,12,16,20,26,27,29,31\}$ 、目的埠 r_2port_d (即 80)及通訊協定編號 r_2p (即 1)作為赫序函數之鍵值(Key)，以分別帶入 2 個赫序函數 h_i 以分別求得下列 32 個(K x W)指向赫序空間 H_{2d} 的位址之集合：

$h_1(0,23,1)=3, h_1(1,23,1)=69, h_1(2,23,1)=30, h_1(3,23,1)=0,$
 $h_1(4,23,1)=56, h_1(7,23,1)=59, h_1(8,23,1)=83, h_1(9,23,1)=46,$
 $h_1(10,23,1)=31, h_1(12,23,1)=47, h_1(16,23,1)=61, h_1(20,23,1)=79,$
 $h_1(26,23,1)=13, h_1(27,23,1)=17, h_1(29,23,1)=28, h_1(31,23,1)=82$

$h_2(0,23,1)=13, h_2(1,23,1)=9, h_2(2,23,1)=82, h_2(3,23,1)=10,$
 $h_2(4,23,1)=109, h_2(7,23,1)=34, h_2(8,23,1)=79, h_2(9,23,1)=22,$
 $h_2(10,23,1)=59, h_2(12,23,1)=111, h_2(16,23,1)=12, h_2(20,23,1)=7,$
 $h_2(26,23,1)=109, h_2(27,23,1)=107, h_2(29,23,1)=3, h_2(31,23,1)=55$

依上述 32 個指向赫序空間 H_{2d} 的位址之集合，在此赫序空間 H_{2d} 上呈現一第 2 條防火牆規則之目的網段特徵值，並將該赫序空間 H_{2d} 加入前述赫序空間 H 中，即使同一位址之位元值進行加總運算，進而如下所示，在此一赫序空間 $H(H=H+H_{2d})$ 上呈現所有防火牆規則之欲過濾網段特徵值總合：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	1	2	0	2	2	0	0	2	0	2	1	0	6	2	0	0	0	2	0	0	2	3	1	0	0	0	0	0	1	1	1	1
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	1	0	1	0	0	2	2	3	2	1	0	0	1	1	0	0	1	0	1	0	0	1	1	0	1	2	0	3	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	1	1	0	1	0	0	0	0	0	0	3	1	0	2	0	1	2	1	1	0	0	0	2	0	0	0	2	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	1	0	2	1	2	0	0	0	0	0	0	1	1	2	2	3	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0



位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0	0	0	1	0	0	1	1	1	0	0	0	0	0	1	1	1	1
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	1	0	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	0	1	0	0	1	1	0	1	1	0	1	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	1	1	0	1	0	0	0	0	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	1	0	1	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0

一旦該防火牆收到一個欲通過的封包 $p : (pip_s, pport_s, pip_d, pport_d, pp) = (12.0.0.4, 1067, 172.17.23.153, 80, 1)$ 時，處理封包之方法與前述處理防火牆規則類似，即使用相同的 2 個(即 $K=2$)赫序函數 $h_i \{1 \leq i \leq 2\}$ ，以定義一相同大小之赫序空間 $H' = C * K * L = 128$ bit 的記憶空間，且其中每一個位元值清除為 0，如下所示：

赫序空間 H'

[illegible]

自該封包中取出一來源網址 pip_s (即 12.0.0.4)，並將該來源網址轉換成以二進位碼排列如下：

[illegible]

從上述來源網址 pip_s 之二進位碼排列中找尋位元值之"1"的 M' 個相對位址之集合，即： $M'=3, \{b'_0, b'_1, b'_2\}=\{2,26,27\}$

將上述每一二進位碼位元值為"1"之相對位址{2,26,27}、來源埠 $pport_s$ (即 1067)及通訊協定編號 pp (即 1)作為赫序函數之鍵值(Key)，以分別帶入 2 個赫序函數 h_i 以分別求得下列 6 個($K \times M'$)指向赫序空間 H' 的位址之集合：

$$h_1(2,1067,1)=61, h_1(26,1067,1)=10, h_1(27,1067,1)=111$$

$$h_2(2,1067,1)=39, h_2(26,1067,1)=46, h_2(27,1067,1)=12$$

依上述 6 個指向赫序空間 H' 的位址之集合，如下所示，在赫序空間 H_s 上呈現該封包之來源網址特徵值：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

自同一封包中取出一目的網址 pip_d (即 172.17.23.153)，並將該目的網址 pip_d 轉換成以二進位碼排列如下：

位址	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
位元	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0	1

從上述目的網址 pip_d 之二進位碼排列中找尋位元值之"1"的 W' 個相對位址之集合，因此從上可知： $W'=14$ ，是以，該相對位址集合= $\{b'_0, b'_1, b'_2, b'_3, b'_4, b'_5, b'_6, b'_7, b'_8, b'_9, b'_{10}, b'_{11}, b'_{12}, b'_{13}\}=\{0,3,4,7,8,9,10,12,16,20,26,27,29,31\}$

將上述每一二進位碼位元值為"1"之相對位址

$\{0,3,4,7,8,9,10,12,16,20,26,27,29,31\}$ 、目的埠 $pport_d$ (即 80)及通訊協定編號 pp (即 1)作為赫序函數之鍵值(Key)，以分別帶入 2 個赫序函數 h_i 以分別求得下列 28 個($K \times W'$)指向赫序空間 H'_d 的位址集合：

$$\begin{aligned} h_1(0,80,1)=60, \quad h_1(3,80,1)=1, \quad h_1(4,80,1)=107, \quad h_1(7,80,1)=8, \\ h_1(8,80,1)=39, \quad h_1(9,80,1)=61, \quad h_1(10,80,1)=40, \quad h_1(12,80,1)=55, \\ h_1(16,80,1)=83, \quad h_1(20,80,1)=97, \quad h_1(26,80,1)=24, \quad h_1(27,80,1)=66, \\ h_1(29,80,1)=70, \quad h_1(31,80,1)=24 \end{aligned}$$

$$\begin{aligned} h_2(0,80,1)=25, \quad h_2(3,80,1)=33, \quad h_2(4,80,1)=1, \quad h_2(7,80,1)=66, \\ h_2(8,80,1)=51, \quad h_2(9,80,1)=43, \quad h_2(10,80,1)=37, \quad h_2(12,80,1)=13, \\ h_2(16,80,1)=90, \quad h_2(20,80,1)=69, \quad h_2(26,80,1)=22, \quad h_2(27,80,1)=91, \\ h_2(29,80,1)=111, \quad h_2(31,80,1)=121 \end{aligned}$$

依上述 28 個指向赫序空間 H'_d 的位址集合，在赫序空間 H'_d 上呈現該封包之目的網址特徵值。接著收集所有指向赫序空間 H' 的位址集合，將該赫序空間 H'_d 加入前述赫序空間 H'_s 中，即同一位址之位元值進行加總運算，以產生一赫序空間 $H'=H'_s+H'_d$ ，如下所示呈現該封包之所有網址特徵值總合：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	2	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	1	0	2	1	0	0	0	0	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	1	0	0	0	1	0	2	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	2	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	2	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0

將前述封包特徵值總合中屬非"0"的位元值皆改設為"1"，以在赫序空間 H' 上呈現該封包中所有欲檢查網址之特徵值集合：

位址	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位元	0	1	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0
位址	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
位元	0	1	0	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0
位址	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
位元	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0
位址	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
位元	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0

進行運算檢查： $(H \text{ OR } H') \text{ XOR } H$ ，結果發現至少有一位元值不等於"0"，則該封包之網址特徵值集合不在該需過濾之網段特值集合範圍內，即封包 p 一定不滿足前述任一條防火牆規則，因此允許該封包通過該防火牆規則。

是以，本發明之加速封包過濾之方法，係利用一搜尋過濾器在固定的時間內先判斷該封包是否不在防火牆規則所涵蓋的範圍之內，讓非屬範圍內之大量封包，立即可確定為無害之良性封包，故可迅速允許該封包通過防火牆，避免網路壅塞；反之，如屬範圍內之少量封包，即可能為有問題之封包，可配合該防火牆中其他具較高搜查成本之封包過濾器(packet filter)作進一步深度過濾，藉此更可以縮短計算時間，使搜尋效率提昇，而非如習知技術是不論每一封包的好壞多寡皆使用相同的封包過濾器。

雖然本發明以較佳實施例揭露如上，然其並非用以限定本發明，任何熟悉此項技藝者，在不脫離本發明之精神和範圍內，當可做些許更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

為使本發明之上述目的、特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖示，詳細說明如下：

第 1 圖係顯示依據本發明較佳實施例之一種加速封包過濾方法適用於一具防火牆之網路系統中；

第 2 圖係顯示依據本發明較佳實施例之一種產生所有欲過濾網段特徵值集合之方法的流程；

第 3 圖係顯示依據本發明較佳實施例之一種產生封包網址特徵值集合之方法的流程；以及

第 4 圖係顯示依據本發明較佳實施例之一種加速封包過濾方法之運算檢查流程。

【元件代表符號簡單說明】

- | | | | |
|----|-------|----|-------|
| 10 | 網際網路 | 20 | 防火牆 |
| 22 | 防火牆規則 | 24 | 搜尋過濾器 |
| 30 | 區域網路 | | |

操作步驟 S400, S405, S410, S415, S420, S425, S430, S435, S440, S445, S450, S500, S505, S510, S515, S520, S525, S530, S535, S540, S545, S550, S600, S605, S610, S615, S620, S625, S630, S640, S645

拾、申請專利範圍：

1.一種加速封包過濾之方法，用於一網路安全裝置中，包括：

依據該網路安全裝置內至少一用於過濾封包之規則，產生一第一赫序空間，且其上呈現所有欲過濾網段的特徵值集合；

依據該網路安全裝置所收到的至少一封包內容，產生一第二赫序空間，且其上可呈現該封包之網址特徵值集合，該第二赫序空間具有與前述第一赫序空間相同之空間大小；

將該第一赫序空間與該第二赫序空間進行特定的布林運算；以及

依據前述布林運算結果，判斷該封包特徵值集合是否不在該網段特徵值集合之範圍內，以進一步決定是否允許該封包通過該網路安全裝置。

2.如申請專利範圍第1項所示之加速封包過濾之方法，其中該網路安全裝置包括一防火牆，藉使前述規則可預設於該防火牆中。

3.如申請專利範圍第2項所示之加速封包過濾之方法，其中該防火牆包括一搜尋過濾器，係配合該防火牆之規則的封包過濾工作。

4.如申請專利範圍第1項所示之加速封包過濾之方法，其中前述每一條規則之內容至少包括一欲過濾之特定網段。

5.如申請專利範圍第4項所示之加速封包過濾之方法，進一步包括：

將前述每一條規則內之一特定網段轉換成以二位進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一相對位址分別轉換成一指向第一赫序空間之對應位址，藉以取得該特定網段之指向第一赫序空間之對應位址的集合；以及

收集所有指向第一赫序空間之對應位址的集合，可在一第一赫序空間中呈現出所有欲過濾網段之特徵值集合。

6.如申請專利範圍第5項所示之加速封包過濾之方法，進一步包括：將每一前述二位進位碼排列中位元值為"1"之相對位址作為至少一特定赫序函

數之鍵值，以進行赫序運算獲得一指向第一赫序空間之對應位址。

7.如申請專利範圍第 5 項所示之加速封包過濾之方法，進一步包括：依據每一指向第一赫序空間之對應位址的集合，分別對應產生一具特定網段特徵值之第一赫序空間；以及

將每一具特定網段特徵值之第一赫序空間中同一位址之位元值進行加總運算，即可在該第一赫序空間中呈現出所有欲過濾網段之特徵值集合。

8.如申請專利範圍第 1 項所示之加速封包過濾之方法，其中前述每一封包內容至少包括：一欲檢查之網址。

9.如申請專利範圍第 8 項所示之加速封包過濾之方法，進一步包括：將前述每一封包內之特定網址轉換成以二位進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一相對位址分別轉換成一指向第二赫序空間之對應位址，藉以取得該網址之指向第二赫序空間之對應位址的集合；以及

收集所有指向第二赫序空間之對應位址的集合，可在一第二赫序空間中呈現出該封包之網址特徵值集合。

10.如申請專利範圍第 9 項所示之加速封包過濾之方法，進一步包括：將每一前述二位進位碼排列中位元值為"1"之相對位址作為至少一特定赫序函數之鍵值，以進行赫序運算獲得一指向第二赫序空間之對應位址。

11.如申請專利範圍第 9 項所示之加速封包過濾之方法，進一步包括：依據每一指向第二赫序空間之對應位址的集合，分別對應產生一具網址特徵值之第二赫序空間；以及

將每一具網址特徵值之第二赫序空間中同一位址之位元值進行加總運算，即可在該第二赫序空間中呈現出該封包之網址特徵值集合。

12.如申請專利範圍第 1 項所示之加速封包過濾之方法，進一步包括：當該第一赫序空間與該第二赫序空間的布林運算結果中至少一位元值不為

"0"則，則該封包特徵值集合不在該網段特徵值集合之範圍內，即允許該封包通過該網路安全裝置。

13.一種加速封包過濾之方法，用於一網路安全裝置中，其中具有一種產生所有欲過濾網段特徵值集合的方法，包括：

自該網路安全裝置所預設之至少一規則中取出每一欲過濾的特定網段；

將每一欲過濾的特定網段轉換成以二進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一位址分別轉換成一指向一赫序空間之對應位址，藉以取得該特定網段之指向赫序空間之對應位址的集合；以及

收集所有指向赫序空間之對應位址的集合，即可在該赫序空間中呈現出所有欲過濾網段之特徵值集合。

14.如申請專利範圍第 13 項所示之加速封包過濾之方法，進一步包括：將每一前述二位進位碼排列中位元值為"1"之相對位址作為至少一特定赫序函數之鍵值以進行赫序運算，藉以獲得該指向赫序空間之對應位址。

15.如申請專利範圍第 13 項所示之加速封包過濾之方法，進一步包括：依據每一指向赫序空間之對應位址的集合，係分別對應產生一具特定網段特徵值之赫序空間；以及

將每一具特定網段特徵值之赫序空間中同一位址之位元值進行加總運算，即可在該赫序空間中呈現出所有欲過濾網段之特徵值集合。

16.如申請專利範圍第 13 項所示之加速封包過濾之方法，進一步包括：所有指向該赫序空間之對應位址之位元值皆設為"1"，藉以呈現出所有欲過濾網段之特徵值集合。

17.一種加速封包過濾之方法，用於一網路安全裝置中，其中具有一種產生封包網址特徵值集合的方法，包括：

自該網路安全裝置所收到的至少一封包中取出每一欲檢查的特定網址；

將前述每一封包內之特定網址轉換成以二位進位碼排列；

將前述二位進位碼排列中位元值為"1"之每一相對位址轉換成一指向一赫序空間之對應位址，藉以取得該網址之指向赫序空間之對應位址的集合；以及

收集所有指向該赫序空間之對應位址的集合，即可在該赫序空間中呈現出該封包之網址特徵值集合。

18.如申請專利範圍第 17 項所示之加速封包過濾之方法，進一步包括：將每一前述二位進位碼排列中位元值為"1"之相對位址作為至少一特定赫序函數之鍵值，以進行赫序運算獲得一指向赫序空間之對應位址。

19.如申請專利範圍第 17 項所示之加速封包過濾之方法，進一步包括：依據每一指向赫序空間之對應位址的集合，可分別對應產生一具網址特徵值之赫序空間；以及

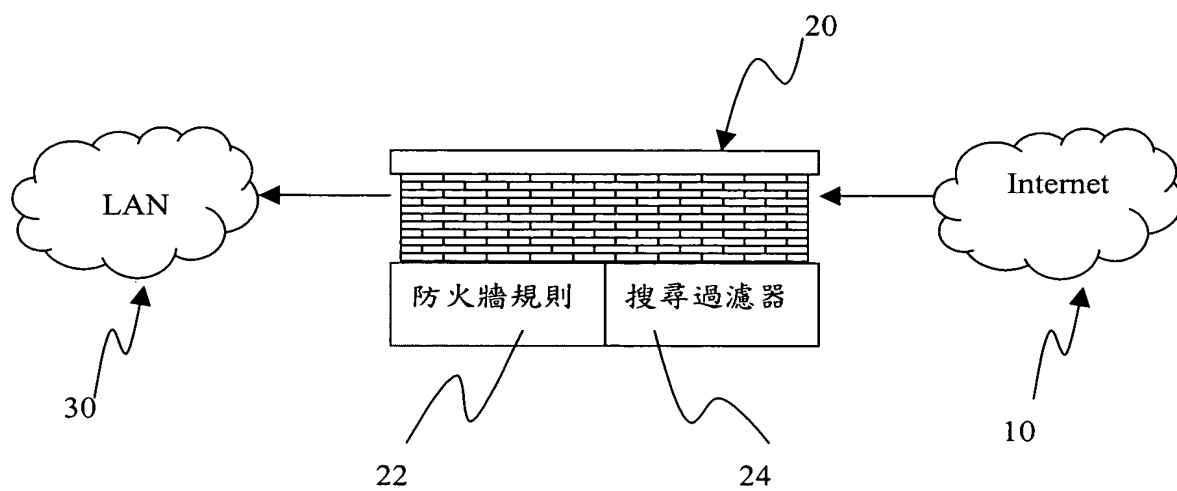
將每一具網址特徵值之赫序空間中同一位址之位元值進行加總運算，即可在該赫序空間中呈現出該封包之網址特徵值集合。

20.如申請專利範圍第 17 項所示之加速封包過濾之方法，進一步包括：將所有指向該赫序空間之對應位址的位元值皆設為"1"，藉以呈現出該封包之網址特徵值集合。

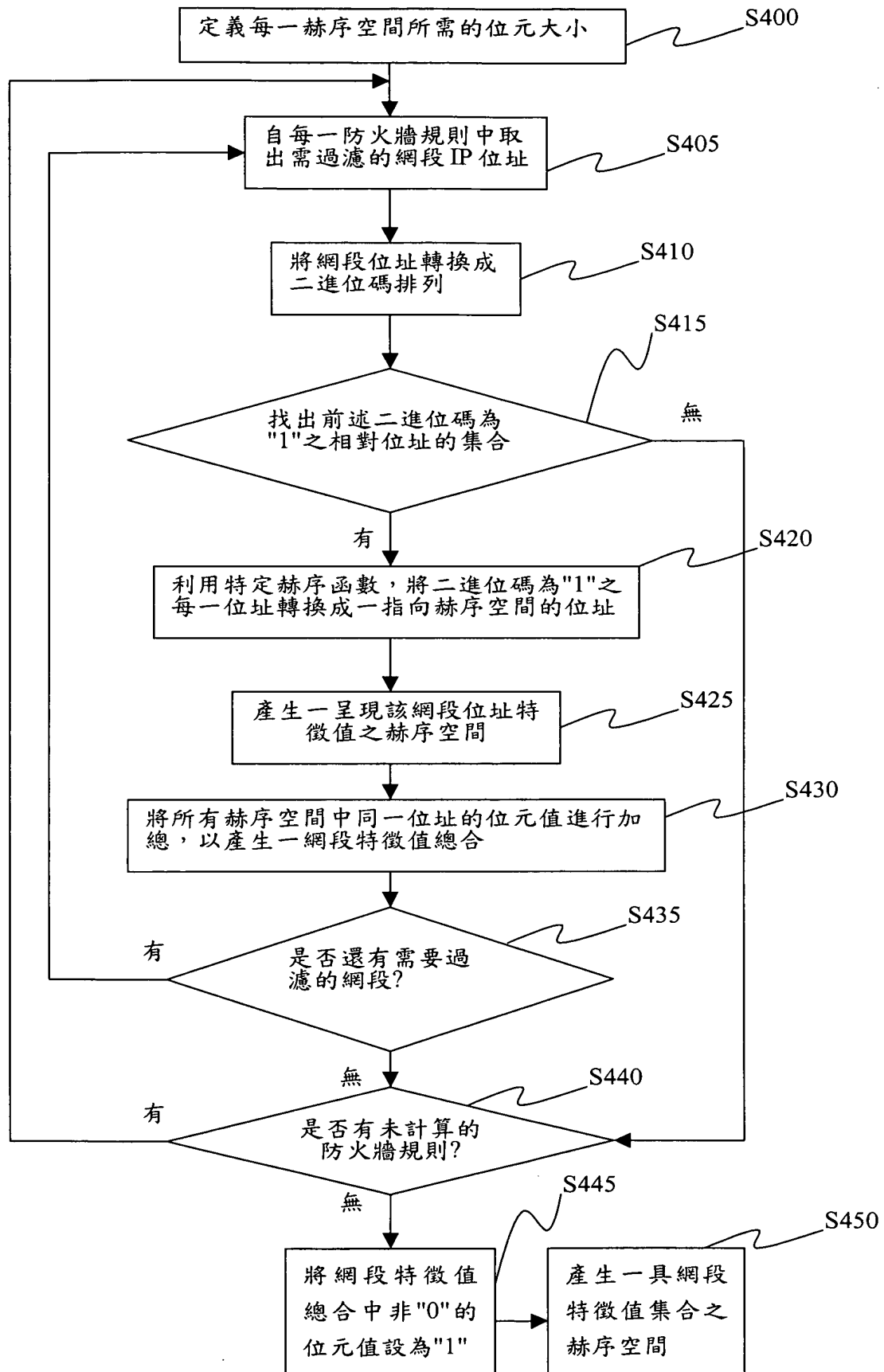
伍、中文發明摘要：

一種加速封包過濾之方法，係以一搜尋過濾器搭配網路防火牆內之規則，該方法包括：依據防火牆規則在一第一赫序空間上呈現所有欲過濾網段的特徵值集合，且依據收到的封包在一第二赫序空間呈現該封包之網址特徵值集合，進而將相同大小的第一及第二赫序空間進行特定的布林運算，一旦結果判斷出該封包特徵值集合不在該網段特徵值集合之範圍內，即迅速允許該封包通過該防火牆，藉此更可以縮短計算時間、降低系統負載及避免網路壅塞。

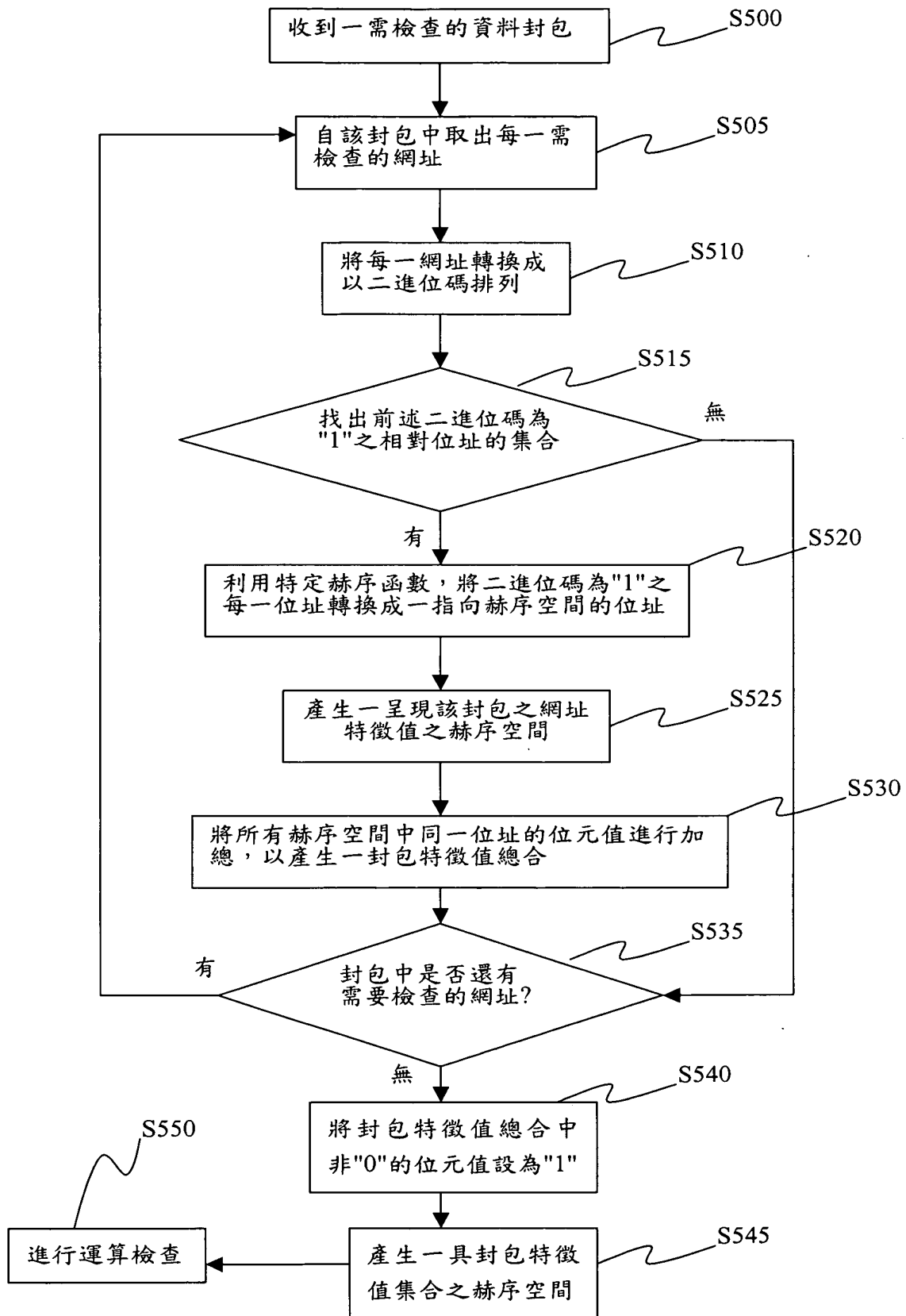
陸、英文發明摘要：



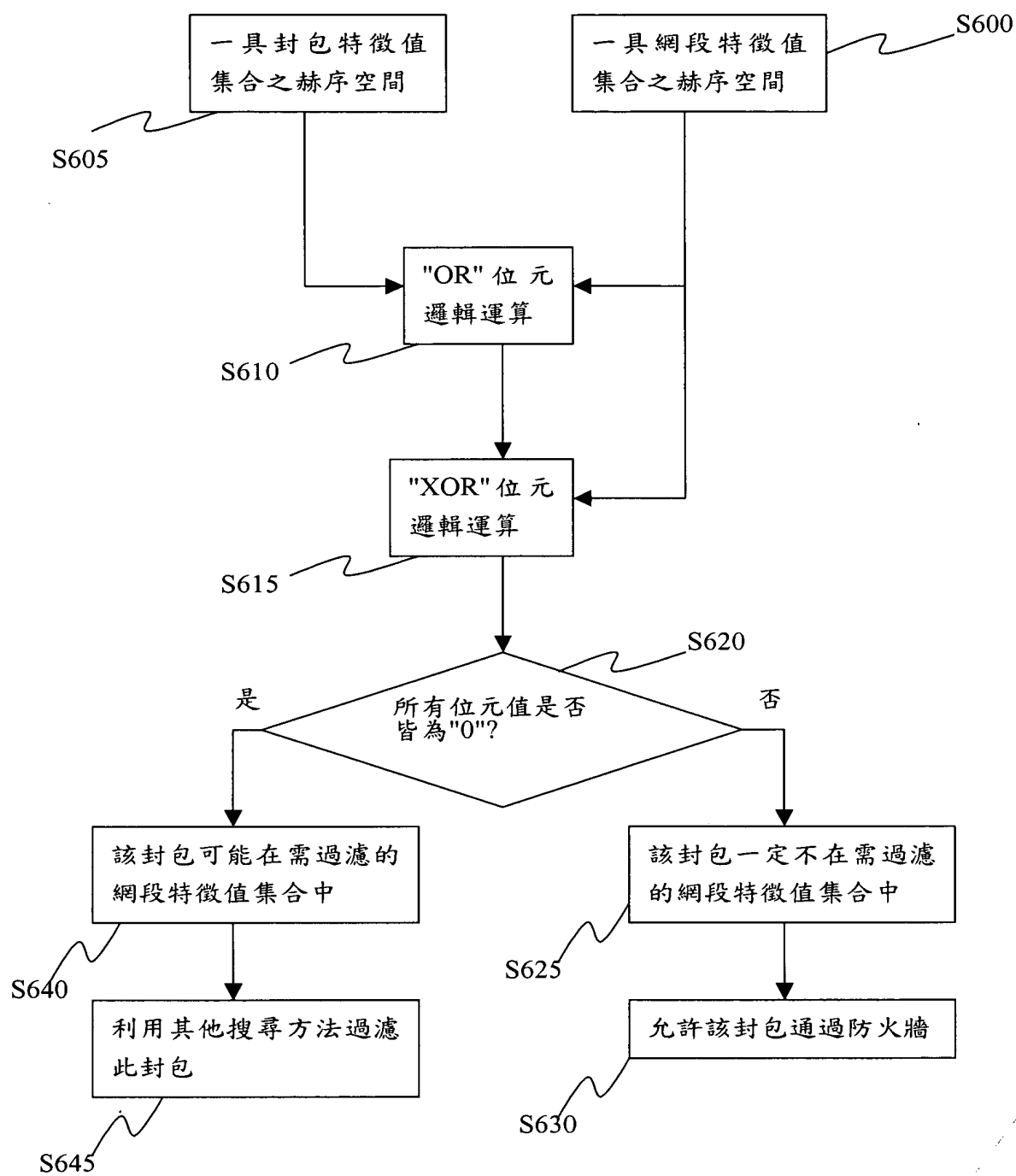
第 1 圖



第 2 圖



第 3 圖



第 4 圖